Advanced Security 1 - CMPU4007
Week 4 - AES

In this lab you are required to provide solutions to the questions below.

AES cipher in ECB mode

Q 1. Modify the programs from the previous lab to work with AES. Write a program to encrypt and decrypt the following with the AES cipher in ECB mode:
key: 1234567812345678
plaintext: AAAABBBBCCCCDDDDAA
plaintext with padding:
AAAABBBBCCCCDDDDAA\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x0014
ciphertext (base 16 encoded):
43D3215C92A75A1478FCF9CB950D20DB502A485FD5735486D57AEA9AA809E3DD

Brute Force

Q 2. Write a program to read a password dictionary file into memory and use the brute force algorithm to iteratively attempt to decrypt the following AES ciphertext from the previous question:
ciphertext (base 16 encoded):
43D3215C92A75A1478FCF9CB950D20DB502A485FD5735486D57AEA9AA809E3DD

Deliverables: Please submit the solved plaintexts, ciphertexts, keys,code and notes written.